REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 06-11-2007	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Military Deception: Transparency in the Information Age

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Edwin J. Grohe

Paper Advisor (if Any): Prof. David Carrington

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
For Example: Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The Information Age has brought about an overwhelming amount of possible intelligence sources. Operational Deception, which grants the operational commander freedom of action, relies on confusing the adversary either through a flood of conflicting information or a supply of incorrect information. There are three main sources of unclassified information that must be accounted for when trying to create this information confusion: commercially available satellite imagery, open source information, and 24/7 media broadcasts. The Operational Commander must make his/her deception effort completely transparent in order to overcome these sources of information and gain the desired reaction from the adversary. Without transparency, and a deception plan rooted in truth, operational deception will be exposed by the adversary and will prove useless.

15. SUBJECT TERMS
Operational Deception, OPSEC, Open Source Information, Commercial Satellite Imagery

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		28	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, RI

Military Deception: Transparency in the Information Age

By
Edwin J Grohe
Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

6 November 2007

Abstract

The Information Age has brought about an overwhelming amount of possible intelligence sources. Operational Deception, which grants the operational commander freedom of action, relies on confusing the adversary either through a flood of conflicting information or a supply of incorrect information. There are three main sources of unclassified information that must be accounted for when trying to create this information confusion: commercially available satellite imagery, open source information, and 24/7 media broadcasts. The Operational Commander must make his/her deception effort completely transparent in order to overcome these sources of information and gain the desired reaction from the adversary. Without transparency, and a deception plan rooted in truth, operational deception will be exposed by the adversary and will prove useless

Table of Contents

INTRODUCTION

In October of 1997, the U.S. Air Force Space Command released a report on Operation Seek Gunfighter, a training exercise conducted to determine whether an aggressor "Red Cell" could successfully track the deployment of an Air Expeditionary Force through open source information and commercially available satellite imagery. The Red Cell was so successful in tracking movement from Mountain Home Air Force Base, Idaho to Bahrain, that analysts were able to determine force structure and identify potential targets.[1] The Air Force determined that "a valuable intelligence picture can be pieced together using a combination of open source information and [commercially available] satellite imagery." [2]

In today's Information Age, there are three sources of readily available information that could be turned into useful intelligence: commercially available satellite imagery, open source information, and 24/7 news media. This paper proposes that the Commander that is successfully able to incorporate these three information sources into a transparent Operational Deception plan will be enabled by their pervasiveness, vice burdened by it. For the purposes of this discussion, transparency will denote a deception plan that employs forces completely available for public view, either through satellite imagery or embedded news reporting.

BACKGROUND

Satellite Technology:

Deception exists on the political, strategic, operational and tactical levels. Operational Deception involves confusing the adversary about an upcoming operation.[3] There are many historical examples of effective Operational Deception. From the Trojan Horse to Operation Fortitude in World War II, commanders have used deception with both great success and outright failure.[4] In the modern age of pervasive, accurate, and instant information, the Operational Commander must think differently about how he or she chooses to employ a deception scheme. The adversary has access to a multitude of information that can essentially negate any deception attempts.

It is also important to distinguish between the state actor and the non-state actor when it comes to planning deception. A state actor may possess a robust intelligence capacity: state owned "spy satellites", HUMINT, SIGINT, and other traditional means of gathering information and turning it into usable intelligence. A non-state actor most probably does not have his or her own covert intelligence organization, but may receive information from friendly third party states. Both state and non-state actors have access to commercial satellite imagery, open source information, and the media. They may use this information to fill in background on intelligence gathered by other means, or as a primary source of information.[5] Either way, the Operational Commander must realize that those sources of information are being used by the adversary, and his or her deception plan must account for the information that the adversary has ready access to.

Deception relies on the human cognitive "See-think-do" process as defined by Joint Publication 3-13.4, *Deception*. This process assesses the actual impact of the deception by the adversary's reaction to it. It assumes that the adversary will see the deceptive action. The "think" and "do" steps are difficult to predict in that some deceptive practices will not cause any action on the part of the adversary. JP 3-13.4 concludes that the enemy must actually take action (or inaction) for a deception to be effective, vice just thinking or perceiving a certain way. [6]

Deception was classified into two categories by Donald Daniel and Katherine Herbig in their 1982 work *Strategic Military Deception*. They differentiated between "A-type" deception which was ambiguity increasing, and "M-type" deception which was misleading. [7] "A-type" would be relatively easy to achieve in the information age; the more information an adversary receives, the more likely it is to be interpreted differently and result in conflicting intelligence reports. "M-type" deception would be one that would disguise the main point of attack or the time and place of an attack.

Satellite Technology:

In addition to countries that possess state owned space imaging systems, commercial satellite technology is both plentiful and capable. The types of imagery available on the market today consist of Electro-optical (EO) images, Synthetic Aperture Radar (SAR), and Multi-Spectral Imagery (MSI) products.[8] The combination of these technologies yield images that are highly capable and have some ability to discern man made objects through "camouflage and counter deception measures."[9]

Two pieces of legislation that are critical to understanding the U.S.'s standing on commercial satellite imagery are Presidential Decision Directive 23 [10] and the Land Remote Sensing Act of 1992.[11] In response to pressure from commercial enterprises, these two items had the combined effect of allowing the commercial development and open market sale of one-meter resolution satellite images. However, these acts also allowed the government to limit U.S. company owned satellite imagery in the name of national defense. The term "Shutter Control" was adopted to describe the U.S. government's ability to control commercial satellite imagery when military operations could be compromised.[12]

In addition to Shutter Control, the U.S. had another path to reduce the impact of commercial satellite company's imaging of U.S. military operations. During the early stages of Operation Enduring Freedom, the Department of Defense (DOD) reached an "assured access" agreement with Space Imaging of Denver. By purchasing all satellite images of Afghanistan for the entire operation, DOD assured the freedom of action for U.S. military forces without the watchful eye of anyone who could afford to buy the images. This "assured access" construct was a more effective way of getting the controversial "shutter control" that the U.S. desired.[13]

Although the Shutter Control has no effect on foreign commercial satellite technology, the initial impact of PDD-23 was to ensure that U.S. companies dominated the commercial satellite imagery market for the foreseeable future. U.S. companies had the lead in the technology at the time. Allowing them to sell their products on the open market was an attempt to prevent foreign entities from entering that market. [14] This dominance, combined with "assured access" would have guaranteed the Operation Commander the ability to avoid detection from commercial imagery systems. However, foreign companies have since entered the market. These commercial enterprises, as well as state owned activities, are rapidly approaching the capabilities of U.S. systems.

Since PDD-23 was signed in 1994, satellite imagery has become more pervasive, timely, and accurate. PDD-23 allowed the commercial release of one meter resolution satellite imagery to replace the two meter and worse imagery of old. [15] The higher the resolution, the more one is able to discern from the image. Now anyone with access to the internet has the availability to look at imagery that is good enough to discern vehicle types, weapon systems, and more. [16] Currently, satellite resolutions of one meter are being eclipsed by even more accurate systems. By the end of the decade, SPOT (Satellite Pour Observation de la Terre) Image will launch the Pleiades imagery system. This system will consist of two spacecraft flying 180 degrees apart. The system will be capable of producing one thousand 0.5-0.7 meter resolution images per day of any part of the Earth. [17] This system, and others like it in development, will present challenges to the Operational Commander. Soon, the Commander must realize that forces in the field will be accurately and rapidly imaged by anyone who has the desire.

Arguably, the development of one meter resolution imagery has had a destabilizing effect on the world balance of power. However, during the Cold War, the U.S. and Soviet capability to image each other's landscape had a stabilizing effect on the balance of power. Each side knew roughly the other's capabilities, force structure and posture. Today, anyone can purchase near real time high resolution imagery. The potential exists for it to be used for targeting and damage assessment. [18]

Some would argue that commercial satellite imagery is more of a force protection issue than an Operation Deception issue. [19] It is true that allowing anyone to look down upon troop concentrations and physical security apparatus present a challenge to the DOD. Currently, free images available on Google Earth are anywhere from one to three years old. [20] This does not present much of a threat to a Commander's ability to execute an operation. However, commercial sources are reducing their delivery timelines toward a 24 hour goal. [21] As technology increases, this timeline will decrease even further, and it won't be long before order to delivery timeline becomes one that could threaten a Commander's freedom of action.

Open Source Information:

"Open source information is publicly available information appearing in print or electronic form. It may be transmitted by radio, television, and newspapers or it may be distributed through commercial databases, images, and drawings."[22] Joint Publication 3-13.3, *Operations Security,* recognizes the importance of open source material to our adversaries, especially terrorist organizations.[23]

The Defense Intelligence Agency started to recognize the value of open source information as early as the 1970s. Much of the information that was being gathered through classified means was readily available through unclassified sources. However, there were no established means of collecting open source information and turning it into intelligence.[24]

The U.S. is not the only one to recognize the importance of Open Source Intelligence (OSINT). The German Federal Intelligence Service (BND) and the New China News Agency (NCNA) use open source information to gather intelligence on foreign powers including the United States.[25] If these states are using open source information, certainly non-state actors without much capacity for covert intelligence gathering are using this material as well.

Currently, the Internet is thought of as being the biggest and most readily available form of OSINT. There are two sets of information available on the internet: Surface information and Deep information. Surface information is readily available through multiple search engines. Deep information is that information which is available only by request. An example of Deep information would be a database that is only available through its own website's search engine.[26] Both of these sources provide a wealth of information. As search engine logic improves, more people will be able to find the information they are looking for without having to wade through hundreds or thousands of documents.

The Department of Defense has measures in place to combat the loss of open source information which may lead to actionable intelligence. DOD Directive 5230.9 *Clearance of DOD Information for Public Release,* and DOD Instruction 5230.29 *Security and Policy Review of DOD Information for Public Release,* provide guidance for the type and amount of information that can be posted to government websites.[27] In addition, each service has its own directives. These policies do not cover non-DOD websites, but a recent crackdown on military bloggers has sparked a trend toward increased OPSEC. The Army has recently undertaken a campaign to inform troops of the rights and wrongs of blogging. Multi-National Corps Iraq (MNC-I) issued policy #9 which addresses content appropriate for posting to unit and personal websites.[28] The Army has also created a power point presentation entitled "OPSEC in the Blogosphere," available on Army Knowledge On-line.[29]

The amount of open source information available is staggering. Turning it into actionable intelligence is a completely different undertaking. One can peruse military blogs, command websites, professional journals such as Jane's and Joint Forces Quarterly, and forums such as SailorBob.com and

AirWarriors.com. These are just a few of the thousands of sources of information available to potential adversaries. The Operational Commander must realize that even day to day life of the U.S. military is posted somewhere on the internet by a technologically advanced junior enlisted or officer.

Role of the Media:

Besides in Internet, open source information has another form: 24 hour news broadcasts. The global market for 24 hour news broadcast has exploded since the Cable News Network became popular back in the 1980's.[30] After Operation Desert Storm, "it was revealed that the Iraqis used CNN coverage as a near real-time intelligence system".[31] In today's current age, not only do reporters get information from the troops they are embedded with, but they also receive daily briefings from trained Public Affairs Officers.

In a controversial move, the Department of Defense is attempting to combine Public Affairs with Information Operations to make Strategic Communications more effective. In 2004, U.S. Central Command established the Office of Strategic Communications to align the messages of Public Affairs and Information Operations.[32] By policy and practice, Public Affairs must tell the truth.[33] Many hold the opinion that information put out by the government must be truthful; otherwise the United States is no better than the adversary. Some may argue that truthfulness is diametrically opposed to deception, which falls under the purview of Information Operations. There were many that opposed the alignment of the two offices based on the premise that each had a different audience and intent, and should therefore be separate.[34] However, in transparent deception, there would be benefit gained from an aligned public message.

Brigadier General Erv Lessel, the first head of strategic communications in Iraq broke information dissemination down into four levels. Public Affairs Officers only concern themselves with the first level of dissemination: giving information to the media. Information Operations concentrates on the second, third and fourth levels. The second level is getting the information to the public. The third level is the target audience absorbing the information. Finally, the fourth level is the target audience taking a specific action or omitting a specific action because of that information.[35]

Since Public Affairs mostly concentrates on U.S. domestic audience and Information Operations concentrates on other audiences, a deception plan would be benefited by incorporating Public Affairs with Information Operations. There should be no reason for either entity to leak incorrect information to the world press, or to plant false stories in the media. In contrast, the deception plan may be aided by highlighting certain truths. For instance, if reporters are embedded with what will be a diversionary force, then the strength and apparent readiness of that force would most likely be transmitted through the media. If more media were embedded with the diversion force than the forces that constituted the main point of attack, then the more airplay that force would receive. Either way, in a force on force major engagement, the adversary is going to know that contact with the enemy is imminent. Operational Deception, aided by Information Operations, could conceal the precise timing and location of the main point of attack.

DISCUSSION / ANALYSIS

In the Information Age, there are many sources of information available to the adversary that could reveal a deception plan. Today's Commander must realize that force structure will be imaged, whether by overhead sensors or by embedded media. Force structure will probably be able to be calculated by a combination of open source material and media. Of course, rather than unclassified source of information, there are other aspects of warfare that present a greater threat: Computer Network Attack, Information Assurance, HUMINT, SIGINT, and violations of OPSEC. Technologically advanced nations, such as China, are probably capable of obtaining information through these surreptitious means.

In today's world, covert and overt information sources will sometimes contradict each other. It is important that the Operational Commander not undertake a deception plan that could be completely negated by the loss of "secure" information. A deception plan that accounts for commercial satellite imagery, open source information, and the media, but is exposed by a few people having their unclassified email intercepted will not succeed. Operational Deception is dependent upon Operational Security (OPSEC) and one of its supporting capabilities, Information Assurance (IA). These functions allow the

Commander to keep secret plans secret. Without both OPSEC and IA, Operational Deception will be useless.[36]

Joint Pub 3-13.4, *Deception,* breaks Operational Deception into 6 principles: focus, objective, centralized planning and control, security, timeliness, and integration. Objective involves causing an adversary "to take (or not to take) specific actions."[37] With the wealth of information available to a potential adversary, the massing of forces in a demonstration or a feint would probably have the greatest chance of eliciting a response. Since the force structure will be imaged, the massing of troops in a diversionary attempt can be enabled by the adversary's access to satellite imagery. The unfortunate aspect of a diversionary force is that the force would have to be real. Actual troops would have to be massed in one area and not used at the main point of attack. Additionally, the main point of attack would probably be visible to the enemy as well. However, if the main point was from an unlikely direction, it might be viewed as the diversion instead. Either way, real combat power would have to be used to create the response of the enemy moving his forces to counter.[38] This violates the principle of mass. The operational commander would have to hold forces from the main point of attack to execute an effective deception. However, these diversionary forces could become the operational reserve once the hostilities commence.

Security is the other principle of Operational Deception most affected by the Information Age. A renewed emphasis on OPSEC is not enough assurance that some entity of the diversionary force may reveal the true intent of their employment. In this instance, the Operational Commander must not allow forces to be used in diversion to know that they are being used in a diversion. Forces must believe that they will be used in the manner assumed from their positioning. Some semblance of normalcy must be present in order to enable the deception picture. Normal planning and preparation of the combat force must be executed in order to complete the illusion. [39] This makes the Deception transparent, and makes it more likely to be believed by the adversary. Only the highest commander of the diversion force should know all the details.

There are two examples in recent history that prove the efficacy of Deception in the Information Age; both involve the 2003 invasion of Iraq. In the first example, Saddam Hussein received intelligence about the U.S. invasion from the Russian ambassador in Baghdad. Whether the information he received was actually planted by the U.S. Central Command is beyond the classification of this report. However, there were key points passed by the Russians that aided the U.S.'s deception efforts. The Russians passed that the ground assault would not begin until the Army's 4th Infantry Division was in place. In fact, the 4th ID was still in transit from their planned route trough Turkey to the Kuwait point of debarkation when the assault began. This occurred a week earlier than the Russians predicted. [40] Had Saddam possessed satellite imagery, he may have even been able to track the 4th IDs movements. Additionally, the Russians passed that the movement of U.S. troops into southern Iraq from Kuwait was a diversion vice the main point of attack. The Russians also passed several pieces of information that turned out to be correct, adding to the fog and friction of information overload.[41] "With the avalanche of information coming out of the U.S., the Iraqis reach[ed] a point where all they know is we aren't coming from Mars," says Daniel Kuehl, a professor of information warfare at the National Defense University. "Information overload is a new form of fog or friction."[42]

These examples in particular underscore the need to have a deception plan that is based in fact. Each of previous examples could have been supported by satellite imagery, embedded media (in transit with the 4th ID), and open source information. If the members of the 4th ID thought that the invasion was going to wait for them, then any weblogs, intercepted emails, or phone calls would support that notion.

The second example of deception in the Information Age had to deal with the underlying reasons for the invasion in the first place. Arguably, the United States has the most powerful intelligence capabilities in the world. With all the intelligence capacity that the U.S. possessed, they were unable to correctly assess the state of Saddam's weapons of mass destruction programs despite 12 years of constant monitoring.[43] In this age, when potential U.S. adversaries possess similar capabilities, this is a true testament to the fact that Operational Deception is still possible.

RECOMMENDATIONS

The recommendations developed from this research into the impact of the Information Age on the commander’s ability to execute Operational Deception are twofold. First, the deception must be transparent. All sources of unclassified information (commercial satellite imagery, open source material, and the media) must support the deception. This will involve real combat power being used in an “M-type” (misleading) deception role. Although this is undoubtedly more expensive that placing plywood aircraft and inflatable tanks on an open field; the rewards are greater if the adversary truly reacts in a cooperative manner. The days of disguising the true capabilities of an entity are probably over, particularly on the operational level. To a lesser extent, the days of giving false capability to something that has no real combat power are also gone.

The second lesson learned from this investigation involves the importance of Operational Security. The best practices of OPSEC will still yield some information flow. If the adversary has any true intelligence capability, Computer Network Defense and Information Assurance are paramount. An elaborate deception plan, created with deference to commercial satellite imagery, open source information and the media, cannot be allowed to fail due to inadvertent information leakage.

FINAL REMARKS

The United States is leaning toward a transparency in world affairs. Transparency enables cooperation and trust amongst international partners and even former competitors. The Open Skies Treaty, enacted in 2002, allows the open and unimpeded imaging of signatories' countries. The imaged country may even provide the aircraft used to procure the images.[44] This transparency also has a place in dealing with the Information Age's impact on military operations.

The Operational Commander must take into account all sources of information that an adversary will use to collect intelligence. The availability of commercial satellite imagery, open source information, and 24/7 news media are sources of information increasingly being used as a means of intelligence. Transparency in Operational Deception will ensure that these sources of information support the deception vice expose its true intent. Realistically, an adversary will not be taken by complete surprise in today's Information Age. An adversary will be able to predict with some accuracy that an attack is coming. The Operational Commander can best employ deception to conceal the exact time and main point of attack. Infusing of truth will be the best way to achieve a synergy of classified and unclassified information.

NOTES

[1] U.S. Air Force Space Command, *Operation SEEK GUNFIGHTER – Aggressor Space Applications Project Operational Report* (Colorado Springs, CO: Falcon Air Force Base, 23 January 1998), 2-4, quoted in Larry Grundhauser, "Sentinels Rising – Commercial High Resolution Satellite Imagery and Its Implications for US National Security," *Airpower Journal*, Winter 1998, 61-81, also available online at http://www.airpower.maxwell.af.mil/airchronicles/apj/apj98/ win98/grund.pdf

[2] Ibid.

[3] Donald C. Daniel and Katherine L. Herbig, *Strategic Military Deception,* (Oxford: Pergamon, 1982), 5-7 quoted in Joseph W. Caddell, *Deception 101-Primer on Deception.* Strategic Studies Institute (Carlisle, PA: U.S. Army War College, December 2004), 9.

[4] Ibid, 8.

[5] Dr. Donald L. Madill, PhD, "Producing Intelligence from Open Sources," *Military Intelligence Professional Bulletin* (December 2005): 22-24, http://www.proquest.com (accessed 2 November 2007).

[6] Chairman, U.S. Joint Chiefs of Staff, *Deception,* Joint Publication (JP) 3-13.4 (Washington, DC: CJCS, 13 Jul 06), IV-2.

[7] Joseph W. Caddell, *Deception 101-Primer on Deception.* Strategic Studies Institute (Carlisle, PA: U.S. Army War College, December 2004), 6-7.

[8] Intelligence Threat Handbook, "Open Source Collection," http://www.fas.org/irp/nsa/ioss/threat96/part06.htm (accessed 14 October 2007)

[9] Bill Sweetman, "Imaging from Space – Spatial Awareness: Satellite Imaging Systems Span the Globe," *Jane's International Defence Review,* Vol 40 (May 2007): 51.

[10] *Foreign Access to Remote Sensing Space Capabilities, Presidential Decision Directive/PDD-23 (10 Mar 94)*, http://www.fas.org/irp/offdocs/pdd23-2.htm

[11] *Land Remote Sensing Act of 1992.* Public Law 102-555. 102d Congress, 28 October 1992.

12. Jeff Morris, “RAND: Satellite ‘Shutter control’ not as big an issue as expected,” *Aerospace Daily,* Vol. 204, Iss. 1 (1 October 2002), http://www.proquest.com/ (accessed 31 October 2007).

13. Ibid.

14. Bill Sweetman, “Spy Satellites: The Next Leap Forward,” *Jane’s International Defence Review 30*, no. 1 (1 January 1997): 30.

15. Federation of American Scientists, “Firm Releases Imagery of Area 51,” http://www.fas.org/irp/overhead/groom.htm (Accessed 3 October 2007).

16. Bill Sweetman, “Imaging from Space – Spatial Awareness: Satellite Imaging Systems Span the Globe,” *Jane’s International Defence Review* 40, (May 2007): 46.

17. Michael A Taverna, “Mix and Match,” *Aviation Week & Space Technology* 165, no. 20 (20 November 2006), http://www.proquest.com/ (accessed 3 October 2007).

18. Federation of American Scientists, “Firm Releases Imagery of Area 51,” http://www.fas.org/irp/overhead/groom.htm (Accessed 3 October 2007).

19. Robert Fabian, *Force Protection in An Era of Commercially Available Satellite Imagery: Space Blockade as a Possible Solution*, ADA400933 (Newport, RI: Naval War College, 04 February 2002)

20. Google Earth Help Center, http://earth.google.com/support/ bin/answer.py?answer=21414, accessed 14 October 2007.

21. Bill Sweetman, “Imaging from Space – Spatial Awareness: Satellite Imaging Systems Span the Globe,” *Jane’s International Defence Review,* Vol 40 (May 2007): 50.

22. Director of Central Intelligence, *A Consumer's Guide to Intelligence, PAS 95-00010*, Washington, DC: Central Intelligence Agency, 1995, p. 3 quoted in Intelligence Threat Handbook, “Open Source Collection,” http://www.fas.org/irp/nsa/ioss/threat96/part06.htm (accessed 14 October 2007)

23. Chairman, U.S. Joint Chiefs of Staff, *Operations Security*, Joint Publication (JP) 3-13.3 (Washington, DC: CJCS, 29 June 2006).

24. Dr. Donald L. Madill, PhD, “Producing Intelligence from Open Sources,” *Military Intelligence Professional Bulletin* (December 2005): 19-20, http://www.proquest.com (accessed 2 November 2007).

25. Intelligence Threat Handbook, “Open Source Collection,” http://www.fas.org/irp/nsa/ioss/threat96/part06.htm (accessed 14 October 2007)

26. David A. Umphress, “Diving the Digital Dumpster – The Impact of the Internet on Collecting Open-Source Intelligence,” *Air and Space Power Journal*, Volume 19, no.4. (Winter, 2005): 84.

27. Ibid, 86.

28. LTG John R. Vines, Commander Multi-National Corps – Iraq, *MNC-I Policy #9 – Unit and Soldier Owned and Maintained Websites,* 06 April 2005, http://www.mnf-iraq.com/images/stories/For_The_Troops/bloggers_policy.pdf (accessed 2 November 2007).

29. U.S. Army 1st Information Operations Command, “OPSEC in the Blogosphere,” https://www.us.army.mil/suite/doc/5470570 (accessed 2 November 2007).

30. Turner Broadcasting System, “Corporate History,” http://www.turner.com/about/corporate_history.html (accessed 29 October 2007)

31. Intelligence Threat Handbook, “Open Source Collection,” http://www.fas.org/irp/nsa/ioss/threat96/part06.htm (accessed 14 October 2007)

32. Joshua Kucera, “Military and the Media – Weaponising the Truth?” *Jane’s Defense Weekly* 42, no. 23 (08 June 2005): 23.

33. Karen Sellers (Naval War College Public Affairs Officer), interviewed by the author, 29 October 2007.

34. Joshua Kucera, “Military and the Media – Weaponising the Truth?” *Jane’s Defense Weekly* 42, no. 23 (08 June 2005): 23.

35. Ibid, 23.

36. Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Washington, DC: CJCS, 13 July 2006), II-7.

37. Ibid, I-4.

38. Milan N. Vego, “Operational Deception in the Information Age,” *Joint Forces Quarterly: JFQ,* 30 (Spring 2002): 66.

39. Ibid.

40. Robert Burns, “Report: Russia Fed Saddam Secrets on U.S. Invasion,” *The Star-Ledger (Newark, New Jersey)*, 25 March 2006, http://www.lexis-nexis.com/ (accessed 28 September 2007).

41. Ibid.

42. Ann Scott Tyson, “Hearts, Minds, Leaflets: War’s Psychological Side” *Christian Science Monitor*, 30 January 2003, USA Section.

43. Craig R. Whitney, ed., *The WMD Mirage – Iraq’s Decade of Deception and America’s False Premise for War* (New York, NY: Public Affairs, LLC).

44. James J. Marquardt, “Open Skies and American Primacy,” *Diplomacy and Statecraft* 18, No. 3 (September 2007): 617-639. Also available online at: http://ejournals.ebsco.com/direct.asp?ArticleID=4D138306F062ADA2B76D

BIBLIOGRAPHY

Armed Forces Newswire Service. "Balancing National Security and Commercial Space Less Challenging," Potomac: 25 May 2000, http://www.proquest.com/ (accessed 2 November 2007).

Arndt, Stephanie R. "Marine Bloggers," *Marine Corps Gazette*, Volume 91, Issue 9, Military Module, (September 2007): 9-13

Burns, Robert. "Report: Russia Fed Saddam Secrets on U.S. Invasion." *The Star-Ledger (Newark, New Jersey),* 25 March 2006. http://www.lexis-nexis.com/ (accessed 28 September 2007)

Caddell, Joseph W. *Deception 101 – Primer on Deception.* Carlisle, PA: Strategic Studies Institute, 2005.

Critz, M.R. *Operational Deception.* NWC 4083. Newport, RI: Naval War College, September 1996.

Daniel, Donald C., and Katherine L. Herbig. *Strategic Military Deception.* Oxford: Pergamon, 1982. Quoted in Caddell, Joseph W. *Deception 101 – Primer on Deception.* Carlisle, PA: Strategic Studies Institute, 2005.

Department of Defense. *Clearance of DOD Information for Public Release.* Department of Defense Directive (DODD) 5230.9. Washington, DC: DoD, 15JUL99.

Department of Defense. *Security and Policy Review of DOD Information for Public Release.* Department of Defense Instruction (DODI) 5230.29. Washington, DC: DoD, 6AUG99.

Director of Central Intelligence. *A Consumer's Guide to Intelligence, PAS 95-00010.* Washington, DC: Central Intelligence Agency, 1995, p. 3 quoted in Intelligence Threat Handbook, "Open Source Collection," http://www.fas.org/irp/nsa/ioss/threat96/part06.htm (accessed 14 October 2007)

Fabian, Robert. *Force Protection in An Era of Commercially Available Satellite Imagery: Space Blockade as a Possible Solution*, ADA400933 (Newport, RI: Naval War College, 04 February 2002)

Federation of American Scientists. "Firm Releases Imagery of Area 51," http://www.fas.org/irp/overhead/groom.htm (Accessed 3 October 2007).

Foreign Access to Remote Sensing Space Capabilities. Presidential Decision Directive/PDD-23 (10 Mar 94), http://www.fas.org/irp/offdocs/pdd23-2.htm (accessed 03 October 2007).

Google Earth Community. "Google Acquires Keyhole Corp." http://bbs.keyhole.com/ubb/showflat.php/Cat/0/Number/12563/an/0/page/7 (accessed 29 October 2007).

Google Earth Help Center. http://earth.google.com/support/bin/ answer.py?answer=21414, accessed 14 October 2007.

Grundhauser, Larry K. "Sentinels Rising – Commercial High Resolution Satellite Imagery and Its Implications for U.S. National Security." *Aerospace Power Journal* (Winter 1998), http://www.maxwell.af.mil/ (accessed 2 November 2007).

Hall, Wayne Michael. *Stray Voltage – War in the Information Age.* Annapolis, MD: Naval Institute Press, 2003.

Intelligence Threat Handbook. "Open Source Collection." http://www.fas.org/irp/nsa/ioss/threat96/part06.htm (accessed 14 October 2007)

Land Remote Sensing Act of 1992. Public Law 102-555. 102d Congress, 28 October 1992.

Kucera, Joshua. "Military and the Media – Weaponising the Truth?" *Jane's Defense Weekly* Vol 42, Iss 23 (08 June 2005): 22-25.

Madill, Dr. Donald L. "Producing Intelligence from Open Sources," *Military Intelligence Professional Bulletin*, December 2005, 19-26, http://www.proquest.com/ (accessed 3 November 2007).

Markowski, David A. *Web Magic: A Strategic Imperative in the Information Age.* Monterey, CA: Naval Postgraduate School, June 2005.

Marquardt, James J. "Open Skies and American Primacy," *Diplomacy and Statecraft* 18, No. 3 (September 2007): 617-639.

Metz, Thomas F., Mark W. Garrett, James E. Hutton, Timothy W. Bush. "Massing Effects in the Information Domain." *Military Review.* (October 2006): 103-113.

Michnowicz, Robert G. OPSEC in the Information Age. USAWC Strategy Research Project. Carlisle, PA: U.S. Army War College, 15 March 2006.

Morris, Jeff. "RAND: Satellite 'Shutter Control' Not As Big An Issue As Expected." *Aerospace Daily* 204, no. 1 (1 October 2002), http://www.proquest.com/ (accessed 1 November 2007).

Morris, Jeff. "AF Official: Image Timeliness Next 'Shutter Control' Issue." *Aerospace Daily & Defense Report* 217, no. 27 (10 February 2006), http://www.proquest.com/ (accessed 1 November 2007).

Morris, Jeff. "Copple: Shutter Control Debate to Heat Up as U.S. Loses Edge." *Aerospace Daily* 204, no. 43 (2 Dec 02), http://www.proquest.com/ (accessed 1 November 2007).

National Operations Security Program. National Security Decision Directive Number 298/NSDD-298, 22 January 1988. http://www.fas.org/irp/offdocs/nsdd298.htm (accessed 20 September 07).

Sweetman, Bill. "Spatial Awareness: Satellite Imaging Systems Span the Globe," *Jane's International Defence Weekly* 40, (1 May 2007): 45-51.

Sweetman, Bill. "Spy Satellites: The Next Leap Forward," *Jane's International Defence Weekly* 30, no. 1 (01 January 1997): 26-32.

Taverna, Michael. "Mix and Match." *Aviation Week &Space Technology* 26, no. 20. (20 Nov 06), http://www.proquest.com/ (accessed 2 November 2007).

Turner Broadcasting System, "Corporate History," http://www.turner.com/about/corporate_history.html (accessed 29 October 2007)

Tyson, Ann Scott. "Hearts, minds, leaflets: War's psychological side." *Christian Science Monitor*, 30 January 2003, USA Section.

Umphress, David A. "Diving the Digital Dumpster – The Impact of the Internet on Collecting Open-Source Intelligence," *Air and Space Power Journal*, Volume 19, no.4. (Winter, 2005): 82-91.

U.S. Air Force Space Command. *Operation SEEK GUNFIGHTER – Aggressor Space Applications Project Operational Report* (Colorado Springs, CO:

Falcon Air Force Base, 23 January 1998), 2-4. quoted in Larry Grundhauser, "Sentinels Rising – Commercial High Resolution Satellite Imagery and Its Implications for US National Security," *Airpower Journal*, Winter 1998, 61-81, also available online at http://www.airpower.maxwell.af.mil/ airchronicles/apj/apj98/win98/grund.pdf

U.S. Army. *Operations Security (OPSEC).* Army Regulation (AR) 530-1. Washington, DC: Headquarters Department of the Army, 27 September 2005.

U.S. Army 1st Information Operations Command. "OPSEC in the Blogosphere." Powerpoint. https://www.us.army.mil/suite/doc/5470570 (accessed 2 November 2007).

U.S. Congress. *Using Open-Source Information Effectively: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security*. 109th Congress, 1st Session, 21 June 2005.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Military Deception*. Joint Publication (JP) 3-13.4. Washington, DC: CJCS, 13 July 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-02. Washington, DC: CJCS, 13 June 2007.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Operations Security*. Joint Publication (JP) 3-13.3. Washington, DC: CJCS, 29 June 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Vision 2020* (Washington, DC: CJCS, June 2000).

Vego, Milan N. "Operational Deception in the Information Age." *Joint Forces Quarterly*: *JFQ*, 30, (Spring 2002): 60-66.

Vines, LTG John R, Commander Multi-National Corps – Iraq. *MNC-I Policy #9 – Unit and Soldier Owned and Maintained Websites,* 06 April 2005. http://www.mnf-iraq.com/images/stories/For_The_Troops/ bloggers_policy.pdf (accessed 2 November 2007).

Whitney, Craig R, ed. *The WMD Mirage – Iraq's Decade of Deception and America's False Premise for War,* New York, NY: Public Affairs, LLC, 2005.